TITLE OF THE INVENTION

IMAGE AUTHENTICATION APPARATUS, IMAGE AUTHENTICATION
METHOD, AND IMAGE AUTHENTICATION PROGRAM

5

FIELD OF THE INVENTION

The present invention relates to an apparatus for
examining and authenticating alteration or non-
10   alteration of image data in an image file.

BACKGROUND OF THE INVENTION

Currently, an image authentication system, which
15   examines and authenticates alteration or non-alteration
of image data by using Message Authentication Code
(MAC) data or digital signature data corresponding to
image data in an image file, is proposed. The
conventional image authentication system is disclosed
20   in, e.g., U.S.P. 5,499,294. Note herein that MAC data
is obtained by processing a hash value of image data by
key data that corresponds to a secret key of a
symmetric key cryptography. Digital signature data is
obtained by processing a hash value of image data by
25   key data that corresponds to a private key of a public
key cryptography.

However, the conventional image authentication

system does not provide a user interface that is convenient and easy to use.

SUMMARY OF THE INVENTION

5

The present invention has been proposed in view of the above problem, and has as its object to provide a user with a user interface that is convenient and easy to use.

10   According to the present invention, the foregoing object is attained by providing an image authentication apparatus having control means for controlling a classifying process that classifies each image file into a group corresponding to a type of authentication

15   data in each image file, and a displaying process including a process of displaying in display means data related to each image file in group unit.

Furthermore, the present invention provides an image authentication method comprising: a step of

20   controlling a classifying process that classifies each image file into a group corresponding to a type of authentication data in each image file; and a step of controlling a displaying process including a process of displaying in display means data related to each image

25   file in group unit.

Furthermore, the present invention provides an image authentication program comprising: a step of

controlling a classifying process that classifies each

image file into a group corresponding to a type of

authentication data in each image file; and a step of

controlling a displaying process including a process of

5   displaying in display means data related to each image

file in group unit.

Other features and advantages of the present

invention will be apparent from the following

descriptions taken in conjunction with the accompanying

10   drawings, in which like reference characters designate

the same or similar parts throughout the figures

thereof.

BRIEF DESCRIPTION OF THE DRAWINGS

15

The accompanying drawings, which are incorporated

in and constitute a part of the specification,

illustrate embodiments of the invention and, together

with the description, serve to explain the principles

20   of the invention.

Fig. 1 is a block diagram showing a main

construction of an image authentication system

according to an embodiment of the present invention;

Fig. 2 is a flowchart describing a procedure

25   executed in accordance with an image authentication

program by an image authentication apparatus proposed

by the embodiment of the present invention;

Fig. 3 shows an example of a screen displayed on a display unit; and

Fig. 4 shows an example of a file format of an image file.

5

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

A preferred embodiment of the present invention will now be described in detail in accordance with Figs. 1 to 4.

10   Fig. 1 is a block diagram showing a main construction of an image authentication system 10 according to the embodiment of the present invention.

Referring to Fig. 1, a control unit 101 controls

15   various functions in the image authentication system 10. Memory 102 stores various data processed by the control unit 101. A storage unit 103 is a memory storing an application program, such as an image authentication program 106 and the like. A user

20   interface unit 104 informs the control unit 101 of a user's designation. A display unit 105 displays data supplied by the control unit 101.

Fig. 3 shows an example of a screen generated by the control unit 101 of the present embodiment in

25   accordance with the image authentication program 106.

Referring to Fig. 3, a screen 300 displays a first window 301, a second window 302, and a third

CFM03242/P203-0382

window 303. The screen 300 also displays data

indicative of the total number of files displayed on

the first window 301, second window 302, and third

window 303.

5   The first window 301 displays a list of

information related to an image file that belongs to a

first group. The image file that belongs to the first

group is an image file having MAC (Message

Authentication Code) data as the authentication data

10   for the image data. MAC data is obtained by processing

a hash value of image data by key data that corresponds

to a secret key of a symmetric key cryptography.

The second window 302 displays a list of

information related to an image file that belongs to a

15   second group. The image file that belongs to the

second group is an image file having digital signature

data as the authentication data for the image data.

Digital signature data is obtained by processing a hash

value of image data by key data that corresponds to a

20   private key of a public key cryptography.

The third window 303 displays a list of

information related to an image file that belongs to a

third group. The image file that belongs to the third

group is an image file having neither MAC data nor

25   digital signature data as the authentication data for

the image data.

Fig. 4 shows an example of a file format of an

- 5 -

image file. The image file is constructed with a
header, a body, and a footer. Note that an image file
having no authentication data (a file displayed in the
third window 303) has no footer, or includes a footer
5   having no storage area for authentication data. The
header includes a file name of the image, camera ID
data which specifies a digital camera that has picked
up the image, and thumbnail images. The "other data"
includes information related to an image size (the
10 number of pixels in the horizontal and vertical
directions), the starting position and size of the
body, the starting position and size of the footer, and
so forth. The body stores compressed image data (JPEG-
encoded image data). The "marker" in the footer is
15 information identifying the type of the authentication
data. Accordingly, it is possible to discriminate
whether the authentication data is MAC data or digital
signature data by examining the "marker". The MAC data
is authenticate data obtained by processing a hash
20 value of image data by key data that corresponds to a
secret key of a symmetric key cryptography. The
Digital signature data is authenticate data obtained by
processing a hash value of image data by key data that
corresponds to a private key of a public key
25 cryptography. It should be noted that the maker and
the authenticate data may be stored in the header
instead of in the footer. Furthermore, the marker and

the authenticate data may be embedded in the image data

using a watermark technology.

Fig. 2 is a flowchart describing one of

procedures executed in accordance with the image

5   authentication program 106 by the image authentication

system proposed by this embodiment. Fig. 2 shows

examination procedure executed automatically when a

user selects one or more image files.

Step S201: The control unit 101 determines

10   whether or not a user has operated the user interface

unit 104 and has selected one folder or one or more

files in the storage unit 103. Note that, at this

time, thumbnail image, file name and camera ID, i.e.,

of each selected image file may be displayed. If the

15   thumbnail image, file name or camera ID is displayed

when the user selects the image files, it is possible

for the user to correctly select image files which he

or she want to examine and authenticate. When one

folder or one or more files are selected, the control

20   proceeds to step S202.

Step S202: The control unit 101 decides one

target file from the one or more image files selected

by the user.

Step S203: The control unit 101 determines

25   whether or not authentication data in the target file

is MAC data. This determination, for example, is made

by examining whether or not the maker in the image file

- 7 -

indicates MAC data. When the authentication data is

MAC data, the control proceeds to step S204. When the

authentication data is not MAC data, the control

proceeds to step S208.

5   Step S204: The control unit 101 classifies the

target file into the first group.

Step S205: The control unit 101 examines and

authenticates alteration or non-alteration of the image

data using the image data in the target file and MAC

10   data in the target file. For example, the control unit

101 compares data, which is obtained by converting the

MAC data by predetermined common key data, with a hash

value calculated based on the image data (body),

thereby performing authentication. If a match is

15   found, the control unit 101 determines non-alteration

of the image, but if a match is not found, the control

unit 101 determines alteration of the image.

Step S206: The control unit 101 displays

altogether in the first window 301, thumbnail images of

20   the target file, a file name, a camera ID indicative of

a unique identifier of the digital camera that has

generated the target file, and the result of

authentication indicative of whether or not the image

data in the target file has been altered.

25   Step S207: The control unit 101 displays the

total number of image files that belong to the first

· group in the first window 301, and displays the total

number of image files that belong to the first to third groups in the screen 300.

Step S208: The control unit 101 determines whether or not the authentication data in the target
5   file is digital signature data. When the authentication data is digital signature data, the control proceeds to step S209. When the authentication data is not digital signature data (including in a case where authentication data is not in the target file),
10   the control proceeds to step S213.

Step S209: The control unit 101 classifies the target file into the second group.

Step S210: The control unit 101 examines and authenticates alteration or non-alteration of the image
15   data using the image data in the target file and the digital signature data corresponding to the image data. For example, the control unit 101 compares data, which is obtained by converting the digital signature data in the target image file by predetermined common key data
20   that corresponds to key data of a common key of a public key cryptography, with a hash value calculated based on the image data (body), thereby performing authentication. If a match is found, the control unit 101 determines non-alteration of the image, but if a
25   match is not found, the control unit 101 determines alteration of the image.

Step S211: The control unit 101 displays

altogether in the second window 302, thumbnail images

of the target file, a file name, a camera ID indicative

of a unique identifier of the digital camera that has

generated the target file, and the result of

5   authentication indicative of whether or not the image

data in the target file has been altered.

Step S212: The control unit 101 displays the

total number of image files that belong to the second

group in the second window 302, and displays the total

10   number of image files that belong to the first to third

groups in the screen 300.

Step S213: The control unit 101 classifies the

target file into the third group.

Step S214: The control unit 101 displays

15   altogether in the third window shown in Fig. 3,

thumbnail images of the target file, a file name and so

forth.

Step S215: The control unit 101 displays the

total number of image files that belong to the third

20   group in the third window 303, and displays the total

number of image files that belong to the first to third

groups in the screen 300.

Step S216: The control unit 101 determines

whether or not there is an image file that has yet to

25   be processed. If YES, the control returns to step

S201.

As described above, according to the image

authentication system 10 of the present embodiment, it
is possible to classify an image file designated by a
user in accordance with the type of authentication data
in the image file, and display the information related
5 to the image file altogether in a window provided for
each group. Accordingly, the user can easily be
informed of the type of authentication data in each
image file.

　　Furthermore, according to the image
10 authentication system 10 of the present embodiment, it
is possible to display thumbnail images of the image
file selected by a user, a file name, a camera ID, and
the authentication result altogether. Therefore, the
user can instantly be informed of the information
15 related to the selected image file.

　　Accordingly, the present invention can provide a
user with a user interface that is convenient and easy
to use.

　　The present invention is not limited to the above
20 embodiment and various changes and modifications can be
made within the spirit and scope of the present
invention. Therefore, to apprise the public of the
scope of the present invention, the following claims
are made.

25